Suggestions given to John Halamka as input to HITPC

Privacy and Security Recommendations for Policy Priorities for the HITPC to Address

May 16, 2010

Micky's request for inputs to help him "orchestrate this so that the HITPC is providing policy guidance in synchrony with the HITSC's needs for policy guidance" is most welcome!

Over the past year, the HITSC P&S WG has explored some areas where we see a need for standards and certification criteria, but where we lack a legal requirement or meaningful-use measure to use as the basis for recommendations. I suspect that as the Regional Extension Centers are established, they too will be looking for policy guidance around the following topics, listed in what I believe is priority order.

1. Shoring up HIPAA – The HIPAA Security Rule contains two categories of Implementation Specifications – "Required" (must implement) and "Addressable" (must implement or describe why not, and implement an alternative). Our P&S WG thought it would be useful to revisit the "Addressable" requirements, and ask the question "for an organization who has adopted an EHR and is using it meaningfully," should this implementation specification be "Required?" Of course we don't have the authority to rewrite the Rule, but the HITPC could make these implementation specs "meaningful use" measures – which would at least require those qualified professionals and hospitals requesting meaningful-use funding to implement them. We would request that the HITPC prioritize revisiting the HIPAA Security Rule's "Addressable" implementation specifications from the perspective of meaningful use of an EHR, and consider adopting some of these specifications as "meaningful use" measures. Our P&S WG presented our specific recommendations to the HITSC in August 2009, with the request that they be passed to the HITPC, but they never got filtered down to the P&S Policy WG. So I separately provided our recommendations (twice) to the P&S Policy WG, but due to conflicting priorities, they were never acted upon. I suggest that our recommendations be used to help inform this discussion.
2. Incorporating Best Practices into Existing Standards – Our WG would like to recommend stronger standards in a couple of areas, but we lack a legal or policy foundation to do so. Two examples that we have discussed are:
    a. Access Control – Role-Based Access Control (RBAC) is needed across healthcare operational environments. Indeed, many existing EHRs provide RBAC. But neither the HIPAA Security Rule nor the current meaningful-use measures requires RBAC. We would request that the HITPC consider adopting RBAC as a meaningful-use measure for Stage 2.

    b. Authentication – The HIPAA Security Rule establishes user and entity authentication as a Standard, but does not indicate the minimum strength needed. Strong identity management is the foundation for safe and secure information use and exchange. Access decisions, digital signatures, and audit all depend upon the validity of user identity, and the safety and legitimacy of exchanges between organizations rely on the validity of the identity of the systems involved in the exchange. The P&S WG wanted to recommend a minimum of assurance Level 2 authentication (allows single-factor, with protections), as defined in NIST SP 800-63, but we had no legal or meaningful-use basis for this recommendation. The recently released DEA IFR for e-prescribing controlled substances requires Level 3 (multi-factor with identity verification) authentication. I believe the DEA IFR gives us a legal basis for requiring that EHRs be able to support two-factor authentication. But there are circumstances other than e-prescribing of controlled substance when two-factor authentication might be called for – for example, access "deniable" information such as mental health, substance abuse, HIV/AIDS, etc, and perhaps access to

EHR from the public we. We suggest the HITPC recommend policies around the level of confidence, or assurance (e.g., NIST level), needed to establish the trustworthiness of an authenticated identity (user and entity) established and shared within the NHIN, and codify these policies as meaningful-use measures that certified EHR technology must support.

3. HIE/NHIN Architectural Assumptions. Our P&S WG has had many discussions about the need for some “assumptions” about HIEs participating in the NHIN. For example, we know that some HIEs are building their own clinical repositories – raising many questions regarding privacy consents, transparency, and data integrity. I personally would like to see the Markle Connecting for Health principles of Decentralization and Federation translated into NHIN policy. At the very least, perhaps the HITPC could address consumer transparency, patient consent, and accountability policies around potential HIE architectures, particularly those that build and maintain their own clinical repositories.
4. Clarification of 2013-2015 Needs for Segmented Data – “Segmentation” is a priority established by ARRA, and the ONC has contracted with George Washington University to study segmentation needs. The HITPC will need to translate this work into policy.
5. Clarification of Consent Exchanges – The standardization efforts currently under way in HL7 and OASIS (in particular – there are others) are designed to accommodate consumer consent rules at a very granular level. For example, “Do not disclose my lab results from May 14 to my neighbor, Jessica Smith.” I personally do not believe consent rules at this level of granularity is practical within an HIE/NHIN. We need policy to establish the level of consent granularity needed between entities in the NHIN.